RELATIVE GALOIS MODULE STRUCTURE OF RINGS OF INTEGERS OF ABSOLUTELY ABELIAN NUMBER FIELDS

HENRI JOHNSTON

ABSTRACT. Let L/K be an extension of number fields where $L/\mathbb{Q}$ is abelian. We define such an extension to be Leopoldt if the ring of integers $\mathcal{O}_L$ of L is free over the associated order $\mathcal{A}_{L/K}$. Furthermore we define an abelian number field K to be Leopoldt if every finite extension L/K with $L/\mathbb{Q}$ abelian is Leopoldt in the sense above. Previous results of Leopoldt, Chan & Lim, Bley, and Byott & Lettl culminate in the proof that the n-th cyclotomic field $\mathbb{Q}^{(n)}$ is Leopoldt for every n. In this paper, we generalize this result by giving more examples of Leopoldt extensions and fields, along with explicit generators.

1. INTRODUCTION

Let L/K be a finite Galois extension of number fields with Galois group G. Then the group algebra $K[G]$ operates on the additive structure of L in the obvious way and we define the associated order of the extension L/K to be

$$\mathcal{A}_{L/K} := \{x \in K[G] \,|\, x(\mathcal{O}_L) \subseteq \mathcal{O}_L\},$$

where $\mathcal{O}_L$ is the ring of integers of L. A natural problem that arises in Galois module theory is that of determining the associated order $\mathcal{A}_{L/K}$ and the structure of $\mathcal{O}_L$ as an $\mathcal{A}_{L/K}$-module.

In the case where $K = \mathbb{Q}$ and $L/\mathbb{Q}$ is abelian, this problem was solved by Leopoldt (see [Leo59]; Lettl gives a simplified proof in [Let90]). In particular, Leopoldt showed that $\mathcal{O}_L$ is a free $\mathcal{A}_{L/\mathbb{Q}}$-module (necessarily of rank 1) and gave explicit descriptions of $\mathcal{A}_{L/\mathbb{Q}}$ and of $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{A}_{L/\mathbb{Q}} \cdot \alpha$.

In the same situation ($K = \mathbb{Q}$ and $L/\mathbb{Q}$ abelian), one can ask whether $\mathcal{O}_L$ has a normal integral basis, i.e. whether it is free as a $\mathbb{Z}[G]$-module (again, necessarily of rank 1). The Hilbert-Speiser Theorem says that this is the case if and only if L is of square-free conductor or, equivalently, the extension $L/\mathbb{Q}$ is tamely ramified. In the more general setting, Noether showed that $\mathcal{A}_{L/K} = \mathcal{O}_K[G]$ precisely when the extension L/K is at most tamely ramified (see [Noe32]). Furthermore, $\mathcal{A}_{L/K}$ is the only order of $K[G]$ over which $\mathcal{O}_L$ can possibly be free of rank 1. Hence Leopoldt's Theorem can be viewed as a generalization of the Hilbert-Speiser Theorem.

A number field K is called a Hilbert-Speiser field if each at most tamely ramified finite abelian extension L/K has a relative normal integral basis, i.e. $\mathcal{O}_L$ is a free $\mathcal{O}_K[G]$-module. In [GRRS99], Greither, Replogle, Rubin and Srivastav show that $\mathbb{Q}$ is the only such number field. In this paper, we consider an analogous problem in which the restriction on ramification is relaxed and the requirement that L/K is abelian is strengthened.

Definition 1.1. An extension L/K of absolutely abelian number fields (i.e. $L/\mathbb{Q}$ abelian) is *Leopoldt* if $\mathcal{O}_L$ is a free $\mathcal{A}_{L/K}$-module. An abelian number field K is *Leopoldt* if every extension L/K with $L/\mathbb{Q}$ abelian is Leopoldt in the sense above.

In particular, Leopoldt's Theorem shows that $\mathbb{Q}$ is Leopoldt. However, unlike the case of Hilbert-Speiser fields, $\mathbb{Q}$ is not the only such field. A series of successively sharper results of Chan & Lim, Bley, and Byott & Lettl (see [CL93], [Ble95] and [BL96], respectively) culminates in the proof that the n-th cyclotomic field $\mathbb{Q}^{(n)}$ is Leopoldt for every n. In [Góm96], Gómez Ayala shows that any quadratic extension L/K with L of p-power conductor over $\mathbb{Q}$ (p an odd prime) is Leopoldt (also see [Let94]). In this paper, we build upon these results by proving the following theorems.

Theorem 1.2. *Let $r, s \geq 1$ and p be an odd prime. Let L/K be an extension with $[L : K] = p^s$ and $L \subseteq \mathbb{Q}^{(p^{r+s})}$. Then L/K is Leopoldt.*

Theorem 1.3. *Let $r \geq 1$, $s \geq 0$ and p be an odd prime. Then $\mathbb{Q}^{(p^{r+s})}/\mathbb{Q}^{(p^r)+}$ is Leopoldt.*

Theorem 1.4. *Let $m \in \mathbb{N}$ with prime factorization $m = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ where $p_1 = 2$ and $r_1 \neq 1$. Let K be the compositum of the collection of number fields $\{K_i\}_{i=1}^k$ where $K_i = \mathbb{Q}^{(p^{r_i})}$ or $\mathbb{Q}^{(p^{r_i})+}$ for $i \geq 2$ and $K_1 = \mathbb{Q}^{(2^{r_1})}$. Then K is Leopoldt.*

Note that these results can be made explicit (see Theorems 8.2 and 9.2). In other words, for a Leopoldt extension L/K we can give an explicit generator $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{A}_{L/K} \cdot \alpha$.

Theorem 1.4 follows from Theorems 1.2 and 1.3 (plus certain cases of the already known results mentioned above) in a relatively straightforward manner as shown in Section 2. One important tool used in the proof of Theorems 1.2 and 1.3 is the result of [Let98] in which Lettl shows that for any finite extension of p-adic fields $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ where $L_{\mathfrak{P}}/\mathbb{Q}_p$ is abelian, $\mathcal{O}_{L_{\mathfrak{P}}}$ is a free $\mathcal{A}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$-module. We then use Roiter's Lemma (see 31.6 of [CR81]) to reduce the problem to the computation of certain discriminants, which we do by explicitly calculating resolvents.

It is natural to ask whether every finite abelian extension of $\mathbb{Q}$ is Leopoldt. One can trivially deduce that the answer is no from results of Brinkhuis ([Bri87], [Bri92], [Bri94]) or Cougnard ([Cou01]), which give many examples of absolutely abelian tame extensions that have no relative normal integral basis. In analogy with the result that $\mathbb{Q}$ is the only Hilbert-Speiser field ([GRRS99]), we would ultimately like to give a classification of all Leopoldt fields. This is a problem that might be explored in a future paper.

2. Piecing Extensions Together

We show that Theorem 1.4 follows from Theorems 1.2 and 1.3, plus Leopoldt's original theorem along with a special case (2-power conductor) of its previously known relative generalizations.

Lemma 2.1. *Let L_1 and L_2 be finite Galois extensions of a number field K. Put $L = L_1 L_2$ and suppose that L_1 and L_2 are arithmetically disjoint over K (i.e. $\mathcal{O}_L = \mathcal{O}_{L_1} \otimes_{\mathcal{O}_K} \mathcal{O}_{L_2}$, or equivalently, L_1 and L_2 are linearly disjoint over K and $(\mathrm{Disc}(\mathcal{O}_{L_1}/\mathcal{O}_K), \mathrm{Disc}(\mathcal{O}_{L_2}/\mathcal{O}_K)) = \mathcal{O}_K$ - see III.2.13 of* [FT91]*). Then:*

(a) *We have $\mathcal{A}_{L/L_2} = \mathcal{A}_{L_1/K} \otimes_{\mathcal{O}_K} \mathcal{O}_{L_2}$ and $\mathcal{A}_{L/K} = \mathcal{A}_{L_1/K} \otimes_{\mathcal{O}_K} \mathcal{A}_{L_2/K}$.*
(b) *If there exists some $\alpha_1 \in \mathcal{O}_{L_1}$ with $\mathcal{O}_{L_1} = \mathcal{A}_{L_1/K} \cdot \alpha_1$, then $\mathcal{O}_L = \mathcal{A}_{L/L_2} \cdot (\alpha_1 \otimes 1)$.*
   If there also exists $\alpha_2 \in \mathcal{O}_{L_2}$ with $\mathcal{O}_{L_2} = \mathcal{A}_{L_2/K} \cdot \alpha_2$, then $\mathcal{O}_L = \mathcal{A}_{L/K} \cdot (\alpha_1 \otimes \alpha_2)$.

Proof. This is Lemma 5 of [BL96]; the proof is immediate. □

Lemma 2.2. *Let L_1/K_1 and L_2/K_2 both be Galois extensions of number fields. Suppose that L_1 and L_2 are arithmetically disjoint over $\mathbb{Q}$ and that for $i = 1, 2$ there exist $\alpha_i \in \mathcal{O}_{L_i}$ such that $\mathcal{A}_{L_i/K_i} \cdot \alpha_i = \mathcal{O}_{L_i}$. Then $\mathcal{O}_{L_1 L_2} = \mathcal{A}_{L_1 L_2/K_1 K_2} \cdot (\alpha_1 \otimes \alpha_2)$ and*

$$\mathcal{A}_{L_1 L_2/K_1 K_2} = \left(\mathcal{A}_{L_1/K_1} \otimes_{\mathcal{O}_{K_1}} \mathcal{O}_{K_1 K_2} \right) \otimes_{\mathcal{O}_{K_1 K_2}} \left(\mathcal{A}_{L_2/K_2} \otimes_{\mathcal{O}_{K_2}} \mathcal{O}_{K_1 K_2} \right).$$

Proof. We give a slightly modified version of the proof dealing with the cyclotomic case given in Section 5 of [CL93]. Consider the following field diagram.
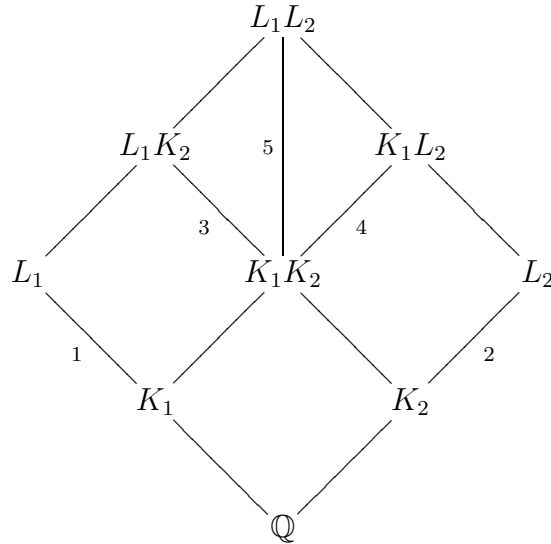
The hypothesis that L_1 and L_2 are arithmetically disjoint over $\mathbb{Q}$ implies that the relevant pairs of fields are arithmetically disjoint over the relevant base field throughout.

We use Lemma 2.1 to move from extensions (1) and (2) to (3) and (4) respectively, and again to arrive at the result for extension (5). □

Proposition 2.3. *Let L/K be an extension of number fields. Then $\mathrm{Tr}_{L/K}(\mathcal{O}_L)$ is an ideal of $\mathcal{O}_K$. Suppose further that L/K is Galois and let $\mathfrak{p}$ be a (non-zero) prime of $\mathcal{O}_K$. Then $\mathfrak{p} \mid \mathrm{Tr}_{L/K}(\mathcal{O}_L)$ if and only if $\mathfrak{p}$ is wildly ramified in L/K.*

Proof. See [Jam]. Alternatively, this follows from Lemma 2 in Section 5 of [Frö67] and the fact that the extension of residue fields in question is separable. □

Corollary 2.4. *If L/K is a Galois extension of number fields, then L/K is at most tamely ramified if and only if $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$.*

Corollary 2.5. *Let M/L and N/L be Galois extensions of number fields with $L \subset M \subset N$ and N/M at most tamely ramified. Put $G = \mathrm{Gal}(N/L)$ and $H = \mathrm{Gal}(M/L)$ and let $\pi : L[G] \to L[H]$ denote the L-linear map induced by the natural projection $G \to H$. Suppose that $\mathcal{O}_N = \mathcal{A}_{N/L} \cdot \alpha$ for some $\alpha \in \mathcal{O}_N$. Then $\mathcal{A}_{M/L} = \pi(\mathcal{A}_{N/L})$ and $\mathcal{O}_M = \mathcal{A}_{M/L} \cdot \mathrm{Tr}_{N/M}(\alpha)$.*

Proof. By Corollary 2.4, $\mathrm{Tr}_{N/M}(\mathcal{O}_N) = \mathcal{O}_M$, and so

$$\mathcal{O}_M = \mathrm{Tr}_{N/M}(\mathcal{O}_N) = \mathrm{Tr}_{N/M}(\mathcal{A}_{N/L} \cdot \alpha) = \mathcal{A}_{N/L}(\mathrm{Tr}_{N/M}(\alpha)) = \pi(\mathcal{A}_{N/L}) \cdot \mathrm{Tr}_{N/M}(\alpha).$$

(Note that the statement and proof are essentially the same as for Lemma 6 of [BL96].) □

Proof of Theorem 1.4. Recall that K is the compositum of the collection of number fields $\{K_i\}_{i=1}^k$ where $K_i = \mathbb{Q}^{(p^{r_i})}$ or $K_i = \mathbb{Q}^{(p^{r_i})+}$ for $i \geq 2$ and $K_1 = \mathbb{Q}^{(2^{r_1})}$ ($p_1 = 2$ and $r_1 \neq 1$), and that we wish to show that K is Leopoldt. In other words, given a finite extension L/K with $L/\mathbb{Q}$ abelian, we need to find $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathcal{A}_{L/K} \cdot \alpha$.

Let $n = p_1^{r_1+s_1} p_2^{r_2+s_2} \cdots p_k^{r_k+s_k}$ be the prime factorization of the conductor of L. Note that we may have $r_i = 0$ for some i. For $1 \leq i \leq k$, let $L_i = \mathbb{Q}^{(p_i^{r_i+s_i})}$. For each $1 \leq i \leq k$, there exists $\beta_i \in \mathcal{O}_{L_i}$ such that $\mathcal{O}_{L_i} = \mathcal{A}_{L_i/K_i} \cdot \beta_i$. We see this as follows: for $r_i = 0$ (i.e. $K_i = \mathbb{Q}$), use Leopoldt's original theorem (see [Leo59] or the simplified proof in [Let90]); for $i = 1$ and $r_1 \geq 2$ use a special case of the main result of [CL93] (or its generalizations in [Ble95] or [BL96]); and for all remaining cases, use Theorems 1.2 and 1.3. Successive applications of Lemma 2.2 give $\mathcal{O}^{(n)} = \mathcal{A}_{\mathbb{Q}^{(n)}/K} \cdot \beta$ where $\beta = \beta_1 \beta_2 \cdots \beta_k$. If n is odd or if $\mathbb{Q}(i) \subseteq K$, then $\mathbb{Q}^{(n)}/L$ is at most tamely ramified (see Proposition 3.7 and Remark 3.8 of [Joh06]) and so we have $\mathcal{O}_L = \mathcal{A}_{L/K} \cdot \mathrm{Tr}_{\mathbb{Q}^{(n)}/L}(\beta)$ by Corollary 2.5.

Now suppose n is even and that $\mathbb{Q}(i) \not\subseteq K$. Then $r_1 = 0$ (recall $p_1 = 2$). Assuming the notation and results of Sections 2 and 3 of [Joh06], let X be the group of Dirichlet characters associated to L, and let L' be the field associated to X_2. Then by Leopoldt's original theorem, there exists $\gamma_1 \in \mathcal{O}_{L'}$ such that $\mathcal{O}_{L'} = \mathcal{A}_{L'/\mathbb{Q}} \cdot \gamma_1$. Let $t = p_2^{r_2+s_2} \cdots p_k^{r_k+s_k}$. As in the odd case, there exists $\gamma_2 \in \mathcal{O}^{(t)}$ such that $\mathcal{O}^{(t)} = \mathcal{A}_{\mathbb{Q}^{(t)}/K} \cdot \gamma_2$. So by Lemma 2.1 we have $\mathcal{O}_{L'\mathbb{Q}^{(t)}} = \mathcal{A}_{L'\mathbb{Q}^{(t)}/K} \cdot \gamma_1 \gamma_2$. However, the extension $L'\mathbb{Q}^{(t)}/L$ is at most tamely ramified (for primes above odd rational primes, use Proposition 3.7 of [Joh06]; for primes above 2, use Theorem 3.5 of [Was97]), and so by Corollary 2.5, we have $\mathcal{O}_L = \mathcal{A}_{L/K} \cdot \mathrm{Tr}_{L'\mathbb{Q}^{(t)}/L}(\gamma_1 \gamma_2)$. □

Remark 2.6. Using the proof above and the results to which it refers, one can give explicit descriptions of α and $\mathcal{A}_{L/K}$. Note, however, that there are in fact many possible choices for α: if $\mathcal{O}_L = \mathcal{A}_{L/K} \cdot \alpha$, then for any unit u of $\mathcal{A}_{L/K}$, we have $\mathcal{O}_L = \mathcal{A}_{L/K} \cdot (u \cdot \alpha)$.

Remark 2.7. Theorem 1.4 can be easily extended using Lemma 2.2 to "add on" non-cyclotomic extensions of the form described in Theorem 1.2 (in the proof above, we only use the cyclotomic case of Theorem 1.2) and quadratic extensions of the forms described in [Góm96] and [Let94]. However, the resulting statement would then be rather messy as it would be about certain Leopoldt extensions rather than Leopoldt fields.

3. From Local Freeness to Global Freeness

Throughout this section, let L/K be a Galois extension of number fields with $G = \mathrm{Gal}(L/K)$ (not necessarily abelian). It is well-known that the ring of integers $\mathcal{O}_L$ being locally free over the associated order $\mathcal{A}_{L/K}$ is a necessary but not a sufficient condition for $\mathcal{O}_L$ to be free over $\mathcal{A}_{L/K}$. However, the proposition below says that in some sense local freeness is "not too far" from global freeness.

Let $[A : B] = [A : B]_{\mathcal{O}_K}$ denote the $\mathcal{O}_K$-module index of B in A. (In fact, one could instead set $[A : B] = [A : B]_{\mathcal{O}_F}$ for any subfield F of K.) For background material on module indices and discriminants, see Sections II.4 and III.2 of [FT91].

Proposition 3.1. *Suppose $\mathcal{O}_L$ is locally free over $\mathcal{A}_{L/K}$. Then given any non-zero ideal I of $\mathcal{O}_K$, there exists $\beta \in \mathcal{O}_L$ (depending on I) such that $I + [\mathcal{O}_L : \mathcal{A}_{L/K} \cdot \beta] = \mathcal{O}_K$.*

Proof. We use Roiter's Lemma as stated in 31.6 of [CR81] (alternatively, see Theorem 27.1 of [Rei75]). Let $R = \mathcal{O}_K$, $\Lambda = M = \mathcal{A}_{L/K}$ and $N = \mathcal{O}_L$. Both M and N are Λ-lattices and are in the same genus since $\mathcal{O}_L$ is locally free over $\mathcal{A}_{L/K}$. Roiter's Lemma says that there exists a Λ-exact sequence

$$0 \to M \to N \to T \to 0$$

for some Λ-module T such that $I + \mathrm{ann}_R(T) = R$. Let S be the image of M in N under the map of the above sequence. Then S is a free Λ-module of rank 1 contained in $N = \mathcal{O}_L$ and so there exists some $\beta \in S \subseteq N = \mathcal{O}_L$ such that $S = \Lambda \cdot \beta = \mathcal{A}_{L/K} \cdot \beta$. Hence we have an exact sequence

$$0 \to \mathcal{A}_{L/K} \cdot \beta \to \mathcal{O}_L \to T \to 0$$

where $I + \mathrm{ann}_{\mathcal{O}_K}(T) = \mathcal{O}_K$. The desired result now follows once one observes that

$$\mathrm{rad}([\mathcal{O}_L : \mathcal{A}_{L/K} \cdot \beta]) = \mathrm{rad}(\mathrm{ann}_{\mathcal{O}_K}(T)).$$

□

The following proposition says that local freeness together with certain extra conditions implies global freeness.

Proposition 3.2. *Suppose that $\mathcal{O}_L$ is locally free over $\mathcal{A}_{L/K}$. Let $\alpha \in \mathcal{O}_L$. Then $\mathcal{O}_L = \mathcal{A}_{L/K} \cdot \alpha$ if and only if $[\mathcal{O}_L : \mathcal{O}_K[G] \cdot \beta] \subseteq [\mathcal{O}_L : \mathcal{O}_K[G] \cdot \alpha]$ for all $\beta \in \mathcal{O}_L$.*

Proof. Let $S = \{\beta \in \mathcal{O}_L \,|\, [\mathcal{O}_L : \mathcal{O}_K[G] \cdot \beta] \neq 0\}$ and observe that this is precisely the set of elements of $\mathcal{O}_L$ that generate a normal basis for the field extension L/K. Note we can assume without loss of generality that $\alpha \in S$. For every $\beta \in S$, the map

$$\psi : K[G] \to L, \quad x \mapsto x \cdot \beta$$

is in fact an isomorphism (in particular, of K-vector spaces) which restricts to an isomorphism of $\mathcal{O}_K$-modules $\mathcal{A}_{L/K} \to \mathcal{A}_{L/K} \cdot \beta$. Thus for every $\beta \in S$, we have

$$[\mathcal{O}_L : \mathcal{O}_K[G] \cdot \beta] = [\mathcal{O}_L : \mathcal{A}_{L/K} \cdot \beta][\mathcal{A}_{L/K} \cdot \beta : \mathcal{O}_K[G] \cdot \beta] = [\mathcal{O}_L : \mathcal{A}_{L/K} \cdot \beta][\mathcal{A}_{L/K} : \mathcal{O}_K[G]].$$

In particular, this holds for $\beta = \alpha$. Hence for all $\beta \in \mathcal{O}_L$ (including $\beta \notin S$) $[\mathcal{O}_L : \mathcal{O}_K[G] \cdot \beta] \subseteq [\mathcal{O}_L : \mathcal{O}_K[G] \cdot \alpha]$ if and only if $[\mathcal{O}_L : \mathcal{A}_{L/K} \cdot \beta] \subseteq [\mathcal{O}_L : \mathcal{A}_{L/K} \cdot \alpha]$. However, $[\mathcal{O}_L : \mathcal{A}_{L/K} \cdot \beta] \subseteq [\mathcal{O}_L : \mathcal{A}_{L/K} \cdot \alpha]$ for all $\beta \in \mathcal{O}_L$ if and only if $[\mathcal{O}_L : \mathcal{A}_{L/K} \cdot \alpha] = (1)$. To see this, note that one direction is trivial and that the other must hold in order to avoid a contradiction with Proposition 3.1. $\square$

We now rephrase Proposition 3.2 in terms of discriminants.

Proposition 3.3. *Suppose that $\mathcal{O}_L$ is locally free over $\mathcal{A}_{L/K}$. Let $\alpha \in \mathcal{O}_L$. Then $\mathcal{O}_L = \mathcal{A}_{L/K} \cdot \alpha$ if and only if for every $\beta \in \mathcal{O}_L$, we have*

$$\mathrm{Disc}((\mathcal{O}_K[G] \cdot \beta)/\mathcal{O}_K) \subseteq \mathrm{Disc}((\mathcal{O}_K[G] \cdot \alpha)/\mathcal{O}_K).$$

Proof. Using a well-known lemma relating discriminants to module indices (see III.2.4 of [FT91]), for all $\beta \in \mathcal{O}_L$ (including $\beta = \alpha$) we have

$$\mathrm{Disc}((\mathcal{O}_K[G] \cdot \beta)/\mathcal{O}_K) = [\mathcal{O}_L : (\mathcal{O}_K[G] \cdot \beta)]^2 \cdot \mathrm{Disc}(\mathcal{O}_L/\mathcal{O}_K).$$

The desired result now follows from Proposition 3.2. $\square$

Proposition 3.4. *Let K be a number field with linearly disjoint extensions L and E. Let $F = LE$ and suppose that F/E (and so L/K) is Galois with Galois group G.*

$$\begin{array}{ccc} & & F \\ & \diagup & \big| \\ L & & \big| \, G \\ \big| \, G & & E \\ & \diagup & \\ K & & \end{array}$$
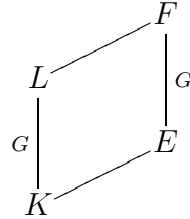
Suppose that $\mathcal{O}_L$ and $\mathcal{O}_F$ are locally free over $\mathcal{A}_{L/K}$ and $\mathcal{A}_{F/E}$ respectively and that there exists $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_F = \mathcal{A}_{F/E} \cdot \alpha$. Then $\mathcal{O}_L = \mathcal{A}_{L/K} \cdot \alpha$.

Proof. First note that the restriction map

$$\mathrm{res} : G = \mathrm{Gal}(F/E) \to \mathrm{Gal}(L/K), \quad \sigma \mapsto \sigma|_L$$

is an isomorphism by the linear disjointness hypothesis. For every $\beta \in \mathcal{O}_L \subseteq \mathcal{O}_F$, we have

$$\mathrm{Disc}((\mathcal{O}_E[G] \cdot \beta)/\mathcal{O}_E) \subseteq \mathrm{Disc}((\mathcal{O}_E[G] \cdot \alpha)/\mathcal{O}_E).$$

However, since $\mathcal{O}_E[G] = \mathcal{O}_E \otimes_{\mathcal{O}_K} \mathcal{O}_K[G]$ we have

$$\mathrm{Disc}((\mathcal{O}_E[G] \cdot \beta)/\mathcal{O}_E) = \mathcal{O}_E \otimes_{\mathcal{O}_K} \mathrm{Disc}((\mathcal{O}_K[G] \cdot \beta)/\mathcal{O}_K)$$

for all $\beta \in \mathcal{O}_L$ (including $\beta = \alpha$). It is now easy to see that

$$\mathrm{Disc}((\mathcal{O}_K[G] \cdot \beta)/\mathcal{O}_K) \subseteq \mathrm{Disc}((\mathcal{O}_K[G] \cdot \alpha)/\mathcal{O}_K)$$

for every $\beta \in \mathcal{O}_L$ and so the desired result now follows from Proposition 3.3.   □

4. RESOLVENTS

In this section, we define resolvents and use them to give a formula for certain discriminants. We then derive a criterion in terms of resolvents for trivial Galois module structure of abelian extensions which will be a key element of the proofs of the main results.

Definition 4.1. For every $k \in \mathbb{N}$ choose a primitive k-th root of unity $\zeta_k \in \mathbb{C}$ in such a way that for all $k, l \in \mathbb{N}$ with $k | l$ we have $\zeta_l^{l/k} = \zeta_k$. Let this choice be fixed for the rest of the paper.

Let L/K be an abelian extension of number fields with Galois group G and let $\widehat{G}$ be the character group of G. Let n be the exponent of G and note that the elements of $\widehat{G}$ can be considered as group homomorphisms $\chi : G \to L(\zeta_n)^\times$.

Definition 4.2. Let $\alpha \in L$ and $\chi \in \widehat{G}$. We define
$$\langle \alpha \,|\, \chi \rangle = \langle \alpha \,|\, \chi \rangle_{L/K} := \sum_{g \in G} \chi(g^{-1}) g(\alpha) \in L(\zeta_n)$$
to be the *resolvent* attached to α and χ.

Proposition 4.3. *Let $\alpha \in \mathcal{O}_L$. Then*
$$\mathrm{Disc}((\mathcal{O}_K[G] \cdot \alpha)/\mathcal{O}_K) = \mathrm{Disc}(\{g(\alpha) : g \in G\}/\mathcal{O}_K) = \prod_{\chi \in \widehat{G}} (\langle \alpha \,|\, \chi \rangle)^2 .$$

Proof. Lemma 5.26 (a) in [Was97] gives $\det((hg^{-1}(\alpha))_{h,g \in G}) = \prod_{\chi \in \widehat{G}} \langle \alpha \,|\, \chi \rangle$ for $\alpha \in L$ (this is known as the abelian group determinant formula). Proposition 2.25 of [Mil] says that $\mathrm{Disc}(\{g(\alpha) : g \in G\}/\mathcal{O}_K) = (\det((hg^{-1}(\alpha))_{h,g \in G}))^2$. Thus we obtain the desired result.   □

Corollary 4.4. *Suppose $\mathcal{O}_L$ is locally free over $\mathcal{A}_{L/K}$. Let $\alpha \in \mathcal{O}_L$. Then*
$$\prod_{\chi \in \widehat{G}} \langle \alpha \,|\, \chi \rangle \;\; divides \;\; \prod_{\chi \in \widehat{G}} \langle \beta \,|\, \chi \rangle \quad \forall \beta \in \mathcal{O}_L$$
if and only if $\mathcal{O}_L = \mathcal{A}_{L/K} \cdot \alpha$. (Note: everything divides zero.)

Proof. Follows from Propositions 3.3 and 4.3.   □

We now give a reduction step useful for computing resolvents.

Lemma 4.5. *Let M be an intermediate field of L/K, $H = \mathrm{Gal}(L/M)$ and $\Delta = \mathrm{Gal}(M/K)$. Suppose χ is a character of G that is trivial on H. Then by abuse of notation we can consider χ as a character on Δ, and for $\alpha \in L$ we have*
$$\langle \alpha \,|\, \chi \rangle_{L/K} = \langle \mathrm{Tr}_{L/M}(\alpha) \,|\, \chi \rangle_{M/K}.$$

Proof. Straightforward.   □

5. Sums of Roots of Unity

We compute certain sums of roots of unity, allowing us to calculate resolvents later on.

Definition 5.1. For any prime p, let $v_p(x)$ denote the p-adic valuation of $x \in \mathbb{Z}$.

Lemma 5.2. *Let p be a prime, $a, b, k \in \mathbb{Z}$ and $k \geq 1$. Then*

$$\sum_{t=0}^{p^k-1} \zeta_{p^k}^{a+bt} = \begin{cases} \zeta_{p^k}^a p^k & \text{if } v_p(b) \geq k, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Straightforward. $\square$

Lemma 5.3. *Let p be a prime, $n, m \geq 1$ ($n \geq 2$ if $p = 2$) and $0 \leq k \leq n+m$. Then*

$$\mathrm{Tr}_{\mathbb{Q}^{(p^{n+m})}/\mathbb{Q}^{(p^n)}}(\zeta_{p^k}) = \begin{cases} \zeta_{p^k} p^m & \text{if } k \leq n, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We have

$$\mathrm{Tr}_{\mathbb{Q}^{(p^{n+m})}/\mathbb{Q}^{(p^n)}}(\zeta_{p^k}) = \sum_{i=0}^{p^m-1} \sigma_{1+ip^n}(\zeta_{p^k}) = \zeta_{p^k} \sum_{i=0}^{p^m-1} \zeta_{p^k}^{ip^n}$$

where σ_i is the automorphism of $\mathbb{Q}(\zeta_{p^{n+m}}) = \mathbb{Q}^{(p^{n+m})}$ mapping $\zeta_{p^{n+m}} \mapsto \zeta_{p^{n+m}}^i$ (and so $\zeta_{p^k} \mapsto \zeta_{p^k}^i$). The result now follows from Lemma 5.2. $\square$

Theorem 5.4 (Gauß). *Let $n \in \mathbb{N}$. Let $\zeta = e^{2\pi i/n}$. Then*

$$\sum_{t=0}^{n-1} \zeta^{t^2} = \begin{cases} \sqrt{n} & \text{if } n \equiv 1 \bmod 4, \\ i\sqrt{n} & \text{if } n \equiv 3 \bmod 4. \end{cases}$$

Proof. See Theorem 99 of [Nag51]. $\square$

Corollary 5.5. *Let p be an odd prime, $k \geq 2$ and $\zeta = \zeta_{p^k}$. Then $\sum_{\substack{0 \leq t \leq p^k-1 \\ (p,t)=1}} \zeta^{t^2} = 0$.*

Proof. Observe that

$$\sum_{t=0}^{p^k-1} \zeta^{t^2} = \sum_{\substack{0 \leq t \leq p^k-1 \\ (p,t)=1}} \zeta^{t^2} + \sum_{t=0}^{p^{k-1}-1} \zeta^{(pt)^2} = \sum_{\substack{0 \leq t \leq p^k-1 \\ (p,t)=1}} \zeta^{t^2} + p \sum_{t=0}^{p^{k-2}-1} \zeta^{p^2 t^2}.$$

The result for now follows by using Theorem 5.4 with $n = p^k$ and $n = p^{k-2}$. (Strictly speaking, we have shown the result for $\zeta = e^{2\pi i/p^k}$, though it is clear that the result still holds for any choice of $\zeta = \zeta_{p^k}$.) $\square$

Proposition 5.6. *Let $F(t) \in \mathbb{Z}_p[t]$, and let α_0 be a simple root of $F(t) \bmod p$. Then there exists a root α of $F(t)$ with $\alpha \equiv \alpha_0 \bmod p$.*

Proof. This is a corollary of Hensel's Lemma - see II.3.25.a of [FT91]. $\square$

Proposition 5.7. *Let p be an odd prime and let $a, b, k \in \mathbb{Z}$ with $k \geq 1$ and $(b, p) = 1$. Let $\zeta = \zeta_{p^k}$ and let $f \in (\mathbb{Z}/p^k\mathbb{Z})[t]$. Define $g : \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ by $t \mapsto a + bt + pf(t)$. Then $\sum_{t=0}^{p^k-1} \zeta^{g(t)} = \sum_{t=0}^{p^k-1} \zeta^{a+bt} = 0$.*

Proof. Since $(b, p) = 1$, we see that g is surjective $\bmod\, p$. Hence Proposition 5.6 shows that g is surjective and therefore bijective. However, $h : \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$, $t \mapsto a + bt$ is also bijective, and so the desired result now follows from Lemma 5.2. □

Corollary 5.8. *Let p be an odd prime and let $a, b, c, d, e, k \in \mathbb{Z}$ with $d, e, k \geq 1$ and $(b, p) = 1$. Let $\zeta = \zeta_{p^k}$ and define $g : \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ by $t \mapsto a + bt + cp \sum_{j=2}^{d} \binom{t}{j} p^{(j-2)e}$. Then $\sum_{t=0}^{p^f-1} \zeta^{g(t)} = 0$.*

Proof. The main point is to check that $f(t) = \sum_{j=2}^{d} \binom{t}{j} p^{(j-2)e}$ is indeed an element of $(\mathbb{Z}/p^k\mathbb{Z})[t]$. One has to consider p-denominators of the binomial coefficients and a straightforward induction argument gives the desired result. □

Proposition 5.9. *Let p be an odd prime and let $a, b, c, k \in \mathbb{Z}$ with $k \geq 0$ and $(c, p) = 1$. Let $\zeta = \zeta_{p^k}$ and let $f \in (\mathbb{Z}/p^k\mathbb{Z})[t]$. Define $g : \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z}$ by $t \mapsto a + bt + ct^2 + pf(t)$. Then $\mathrm{Norm}_{\mathbb{Q}^{(p^k)}/\mathbb{Q}} \left(\sum_{t=0}^{p^k-1} \zeta^{g(t)} \right) = \mathrm{Norm}_{\mathbb{Q}^{(p^k)}/\mathbb{Q}} \left(\sum_{t=0}^{p^k-1} \zeta^{t^2} \right) = p^{\frac{1}{2}k[\mathbb{Q}^{(p^k)}:\mathbb{Q}]} = p^{\frac{1}{2}k(p-1)p^{k-1}}.$*

Proof. Define h to be the first three terms of g, that is $h(t) = a + bt + ct^2$. Since multiplying $g(t)$ by the multiplicative inverse of c in $\mathbb{Z}/p^k\mathbb{Z}$ (recall $(c, p) = 1$) does not affect the norm of $\sum \zeta^{g(t)}$, we can without loss of generality suppose that $c \equiv 1 \bmod p^k$. Thus we have $h(t) = a + bt + t^2$. Now completing the square, we see that there exists a change of variables $x = t - b/2$ such that $h(x) = x^2$. (Note that without loss of generality we can take the constant term to be zero, as again this does not affect the norm.) Thus we have $g(x) = x^2 + pf(x + b/2)$, and since f was arbitrary, we can suppose that in fact $g(x) = x^2 + pf(x)$.

If $k = 0$ or 1, the result now follows from Theorem 5.4 and the fact that $g = h$ in this case (both are defined as functions on $\mathbb{Z}/p^k\mathbb{Z}$). We suppose that $k \geq 2$ and proceed by induction.

Let $H_1 := \{j \in (\mathbb{Z}/p^k\mathbb{Z})^\times \mid 1 \leq (j \bmod p) \leq (p-1)/2\}$, let $H_2 := (\mathbb{Z}/p^k\mathbb{Z})^\times - H_1$ and let $H_3 := (p\mathbb{Z}/p^k\mathbb{Z})$. Note that H_1, H_2 and H_3 form a partition of $(\mathbb{Z}/p^k\mathbb{Z})$, and that the congruence class $\bmod p$ of an element $x \in (\mathbb{Z}/p^k\mathbb{Z})$ uniquely determines the H_i in which it lies. Furthermore, $H_1 = -H_2$ and so both the restrictions $h|_{H_1}$ and $h|_{H_2}$ are bijections onto their common image, $(\mathbb{Z}/p^k\mathbb{Z})^{\times 2}$ (i.e. the squares in $(\mathbb{Z}/p^k\mathbb{Z})^\times$).

Since $g \equiv h \bmod p$ and $g'(x) \equiv 2x \not\equiv 0 \bmod p$ for all $x \in (\mathbb{Z}/p^k\mathbb{Z})^\times$, Proposition 5.6 shows that $g(H_1) = g(H_2) = (\mathbb{Z}/p^f\mathbb{Z})^{\times 2} = h(H_1) = h(H_2)$. Therefore for $i = 1, 2$ we have permutations $s_i : H_i \to H_i$ such that $h|_{H_i}(x) = g|_{H_i}(s_i(x))$. We can "glue" these together to give a permutation $s : (\mathbb{Z}/p^k\mathbb{Z})^\times \to (\mathbb{Z}/p^k\mathbb{Z})^\times$ such that $h(x) = g(s(x))$ for all $x \in (\mathbb{Z}/p^k\mathbb{Z})^\times$. By Corollary 5.5, we now have

$$\sum_{\substack{0 \leq x \leq p^k-1 \\ (p,x)=1}} \zeta^{g(x)} = \sum_{\substack{0 \leq x \leq p^k-1 \\ (p,x)=1}} \zeta^{x^2} = 0 \quad \text{and so} \quad \sum_{x=0}^{p^k-1} \zeta^{g(x)} = \sum_{x=0}^{p^{k-1}-1} \zeta^{g(px)}.$$

Write $f(x) = d + ex + x^2 \tilde{f}(x)$ and let $\tilde{g}(x) = x^2 + ex + px^2 \tilde{f}(px)$. Then we have

$$g(px) = p^2 x^2 + pf(px) = p^2 x^2 + pd + p^2 ex + p^3 x^2 \tilde{f}(px) = pd + p^2 \tilde{g}(x).$$

As before, we can suppose without loss of generality that $d = 0$, and so

$$\sum_{x=0}^{p^k-1} \zeta^{g(x)} = \sum_{x=0}^{p^{k-1}-1} \zeta^{g(px)} = \sum_{x=0}^{p^{k-1}-1} \zeta^{p^2 \tilde{g}(x)} = p \sum_{x=0}^{p^{k-2}-1} \zeta_{p^{k-2}}^{\tilde{g}(x)}.$$

Since $\tilde{g}$ is of the correct form and

$$\sum_{x=0}^{p^k-1} \zeta^{x^2} = \sum_{x=0}^{p^{k-1}-1} \zeta^{(px)^2} = p \sum_{x=0}^{p^{k-2}-1} \zeta_{p^{k-2}}^{x^2},$$

the result now follows by induction. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \square$

Corollary 5.10. *Let p be an odd prime and let $a, b, c, d, e, k \in \mathbb{Z}$ with $d \geq 2$, $e, k \geq 1$, $(c, p) = 1$ (if $p = 3$, assume $e \geq 2$). Let $\zeta = \zeta_{p^k}$ and define*

$$g : \mathbb{Z}/p^k\mathbb{Z} \to \mathbb{Z}/p^k\mathbb{Z} \quad by \quad t \mapsto a + bt + c \sum_{j=2}^{d} \binom{t}{j} p^{(j-2)e}.$$

Then $\mathrm{Norm}_{\mathbb{Q}(p^k)/\mathbb{Q}} \left(\sum_{t=0}^{p^k-1} \zeta^{g(t)} \right) = p^{\frac{1}{2}k(p-1)p^{k-1}}$.

Proof. Write

$$g(t) = a + bt + c\binom{t}{2} + c \sum_{j=3}^{d} \binom{t}{j} p^{(j-2)e} = a + (b - \tfrac{c}{2})t + \tfrac{c}{2}t^2 + cp \sum_{j=3}^{d} \binom{t}{j} p^{(j-2)e-1}.$$

The main point is to check that $f(t) = \sum_{j=3}^{d} \binom{t}{j} p^{(j-2)e-1}$ is indeed an element of $(\mathbb{Z}/p^k\mathbb{Z})[t]$. One has to consider p-denominators of the binomial coefficients and a straightforward induction argument gives the desired result except when $e = 1$ and $p = 3$. $\qquad \square$

6. Absolutely Abelian Extensions

We recall two results for absolutely abelian extensions of number fields. The first of these results says that all absolutely abelian extensions of number fields have the local freeness property which allows the results of Sections 3 and 4 to be applied.

Theorem 6.1 ([Let98]). *Let $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ be a finite extension of p-adic fields with $L_{\mathfrak{P}}/\mathbb{Q}_p$ abelian. Then $\mathcal{O}_{L_{\mathfrak{P}}}$ is a free $\mathcal{A}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$-module of rank 1.*

Corollary 6.2 ([Let98]). *If L/K is an extension of number fields with $L/\mathbb{Q}$ abelian, then $\mathcal{O}_L$ is locally free over $\mathcal{A}_{L/K}$, i.e. for any prime $\mathfrak{p}$ of $\mathcal{O}_K$, $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathcal{A}_{L/K,\mathfrak{p}}$-module of rank 1.*

Let L/K be an extension of number fields with $L/\mathbb{Q}$ abelian and let $G = \mathrm{Gal}(L/K)$. The second result asserts that the associated order $\mathcal{A}_{L/K}$ is equal to $\mathcal{M}_{K[G]}$, the maximal $\mathcal{O}_K$-order of $K[G]$, in many cases of interest. Note that $\mathcal{M}_{K[G]}$ is unique in this case because G is abelian.

Definition 6.3. We say that an extension N/M is *totally wildly ramified* if each intermediate field different from M is wildly ramified above M.

Theorem 6.4 ([BL96]). *Let L/K be a cyclic and totally wildly ramified extension of number fields with $L/\mathbb{Q}$ abelian. Suppose L/K is linearly disjoint from the extension $\mathbb{Q}^{(m)}/K$, where m denotes the conductor of K. Then $\mathcal{A}_{L/K} = \mathcal{M}_{K[G]}$ where $G = \mathrm{Gal}(L/K)$.*

7. The Induction Step

We now specialize to the following situation:

- Let $r, s \geq 1$ and p be an odd prime.
- Let $V = \{x \in \mathbb{Z} : v_p(x) = 0\}$.
- Let $\zeta = \zeta_{p^{r+s}}$.
- Let $L = \mathbb{Q}^{(p^{r+s})}$, $M = \mathbb{Q}^{(p^{r+s-1})}$ and $K = \mathbb{Q}^{(p^r)}$ or $\mathbb{Q}^{(p^r)+}$.
- Let $G = \mathrm{Gal}(L/K)$, $H = \mathrm{Gal}(L/M)$ and $\Delta = \mathrm{Gal}(M/K)$.
- Let A be the subgroup of characters of G that are trivial on H. Note that $A \cong \widehat{\Delta}$.
- Let $B = \widehat{G} - A$. Note that this is the set of characters of G of order p^s or $2p^s$.

Remark 7.1. We shall assume for the rest of the paper that $r \geq \min\{2, s\}$ if $p = 3$ due to the exceptional case of Corollary 5.10 (note that this proposition is only used when $s > r$). However, we already know that extensions of the form $\mathbb{Q}^{(3^{1+s})}/\mathbb{Q}^{(3)}$ are Leopoldt by the main result of [CL93] (or its generalizations in [Ble95] or [BL96]). Furthermore, the only proper subfield of $\mathbb{Q}^{(3)}$ is $\mathbb{Q}^{(3)+} = \mathbb{Q}$, so results analogous to Corollary 8.3 and Theorem 9.2 in the case $p = 3$ and $r = 1$ follow from Leopoldt's original theorem [Leo59] (see [Let90] for a simplified proof). Thus Theorems 1.2 and 1.3 as stated still hold in this case.

Lemma 7.2. *Let σ_i denote the field automorphism of $L = \mathbb{Q}(\zeta)$ defined by $\zeta \mapsto \zeta^i$. Then*

$$G = \mathrm{Gal}(L/K) = \begin{cases} \{\sigma_{1+ip^r} : 0 \leq i \leq p^s - 1\} = \langle \sigma_{1+p^r} \rangle & \text{if } K = \mathbb{Q}^{(p^r)}, \\ \{\sigma_{1+ip^r} : 0 \leq i \leq p^s - 1\} \times \{\sigma_1, \sigma_{-1}\} = \langle \sigma_{-1}\sigma_{1+p^r} \rangle & \text{if } K = \mathbb{Q}^{(p^r)+}. \end{cases}$$

Proof. Straightforward. □

Lemma 7.3. *Let $b \in \mathbb{Z}$ and $\chi \in \widehat{G}$. Then*

$$\langle \zeta^b \,|\, \chi \rangle_{L/\mathbb{Q}^{(p^r)+}} = \begin{cases} \langle \zeta^b \,|\, \chi \rangle_{L/\mathbb{Q}^{(p^r)}} - \langle \zeta^{-b} \,|\, \chi \rangle_{L/\mathbb{Q}^{(p^r)}} & \text{if } \chi \text{ is of even order}, \\ \langle \zeta^b \,|\, \chi \rangle_{L/\mathbb{Q}^{(p^r)}} + \langle \zeta^{-b} \,|\, \chi \rangle_{L/\mathbb{Q}^{(p^r)}} & \text{if } \chi \text{ is of odd order}. \end{cases}$$

Proof. If χ is of even order, we have

$$\begin{aligned} \langle \zeta^b \,|\, \chi \rangle_{L/\mathbb{Q}^{(p^r)+}} &= \sum_{k=0}^{1} \sum_{j=0}^{p^s-1} \chi(((\sigma_{-1})^k (\sigma_{1+p^r})^j)^{-1}) \sigma_{(-1)^k(1+p^r)^j}(\zeta^b) \\ &= \sum_{j=0}^{p^s-1} \chi((\sigma_{1+p^r})^{-j}) \sigma_{(1+p^r)^j}(\zeta^b) - \sum_{j=0}^{p^s-1} \chi((\sigma_{1+p^r})^{-j}) \sigma_{(1+p^r)^j}(\zeta^{-b}) \\ &= \langle \zeta^b \,|\, \chi \rangle_{L/\mathbb{Q}^{(p^r)}} - \langle \zeta^{-b} \,|\, \chi \rangle_{L/\mathbb{Q}^{(p^r)}}. \end{aligned}$$

The calculation is almost identical for χ of odd order.   □

Lemma 7.4. *Let $\chi \in B$ and let $b \in \mathbb{Z}$ with $v_p(b) > 0$. Then $\langle \zeta^b \,|\, \chi \rangle_{L/K} = 0$.*

Proof. Since $\chi \in B$, we have $\chi(\sigma_{1+p^r}) = \zeta^{ap^r}$ for some $a \in V$. Then using Definition 4.2 and noting the explanations below, we have

$$
\langle \zeta^b \,|\, \chi \rangle_{L/\mathbb{Q}^{(p^r)}} \;=\; \sum_{j=0}^{p^s-1} \chi((\sigma_{1+p^r})^{-j})(\sigma_{1+p^r})^j(\zeta^b) = \sum_{j=0}^{p^s-1} \zeta^{-ajp^r} \zeta^{b\sum_{i=0}^{j}\binom{j}{i}p^{ir}}
$$

$$
= \sum_{j=0}^{p^s-1} \zeta^{-ajp^r} \zeta^{b\sum_{i=0}^{\lfloor s/r \rfloor+1}\binom{j}{i}p^{ir}} = \zeta^b \sum_{j=0}^{p^s-1} \zeta^{p^r\left((b-a)j + bp^r \sum_{i=2}^{\lfloor s/r \rfloor+1}\binom{j}{i}p^{(i-2)r}\right)} = 0,
$$

where the last equality follows from Corollary 5.8, noting that $v_p(b - a) = 0$. For the third equality above, note that $\binom{j}{i} = 0$ for $i > j$ and that $p^{ir} \equiv 0 \bmod p^{r+s}$ for $i \geq \lfloor s/r \rfloor + 2$. The $K = \mathbb{Q}^{(p^r)+}$ case now follows from Lemma 7.3.   □

Proposition 7.5. *Suppose there exist $\gamma \in \mathcal{O}_M$, $f \in \mathbb{N}$ and $S \subseteq V$ such that*
  (a) *$\mathcal{O}_M = \mathcal{A}_{M/K} \cdot \gamma$;*
  (b) *for every $\chi \in B$ and every $b \in V$, we have $\mathrm{Norm}_{L/\mathbb{Q}}((\langle \zeta^b \,|\, \chi \rangle_{L/K})) = 0$ or p^f; and*
  (c) *for every $\chi \in B$, there exists a unique element $b = b_\chi \in S$ such that $\langle \zeta^b \,|\, \chi \rangle_{L/K} \neq 0$.*
Then $\mathcal{O}_L = \mathcal{A}_{L/K} \cdot \alpha$ where $\alpha := \gamma + \sum_{b \in S} \zeta^b$.

Proof. Let $\beta \in \mathcal{O}_L$. By Lemmas 4.5 and 5.3, we have

$$
(1) \qquad \prod_{\chi \in A} \langle \alpha \,|\, \chi \rangle_{L/K} = \prod_{\chi \in \widehat{\Delta}} \langle \mathrm{Tr}_{L/M}(\alpha) \,|\, \chi \rangle_{M/K} = \prod_{\chi \in \widehat{\Delta}} \langle p\gamma \,|\, \chi \rangle_{M/K} = p^{|\widehat{\Delta}|} \prod_{\chi \in \widehat{\Delta}} \langle \gamma \,|\, \chi \rangle_{M/K}.
$$

Let $\theta = p^{-1}\mathrm{Tr}_{L/M}(\beta)$. Then $\theta \in \mathcal{O}_M$ by Lemma 5.3. Furthermore, as above, we have

$$
(2) \qquad \prod_{\chi \in A} \langle \beta \,|\, \chi \rangle_{L/K} = p^{|\widehat{\Delta}|} \prod_{\chi \in \widehat{\Delta}} \langle \theta \,|\, \chi \rangle_{M/K}.
$$

However, since $\mathcal{O}_M = \mathcal{A}_{M/K} \cdot \gamma$, Corollary 4.4 shows that (1) divides (2).

Since $\gamma \in \mathcal{O}_M$, we can write $\gamma = \sum_{t \in T} \zeta^{pt}$ for some $T \subset \mathbb{Z}$. Let $\mathfrak{p} = (1 - \zeta)$ be the unique prime ideal in $\mathcal{O}_L = \mathbb{Z}[\zeta]$ above p. Note that $\mathrm{Norm}_{L/\mathbb{Q}}(x) = p^f$ is equivalent to $(x) = \mathfrak{p}^f$ for any $x \in \mathcal{O}_L$. Therefore by Lemma 7.4 and hypotheses (b) and (c), we have

$$
(3) \qquad \prod_{\chi \in B} \langle \alpha \,|\, \chi \rangle_{L/K} = \prod_{\chi \in B} \langle \textstyle\sum_{t \in T} \zeta^{pt} + \sum_{b \in S} \zeta^b \,|\, \chi \rangle_{L/K}
$$

$$
= \prod_{\chi \in B} \langle \textstyle\sum_{b \in S} \zeta^b \,|\, \chi \rangle_{L/K} \text{ generates } \mathfrak{p}^{f|B|}.
$$

Similarly, we can write $\beta = \sum_{t \in T'} \zeta^{pt} + \sum_{s \in S'} \zeta^s$ for some $S' \subseteq V$ and $T' \subseteq \mathbb{Z}$. Then

$$
(4) \qquad \prod_{\chi \in B} \langle \beta \,|\, \chi \rangle_{L/K} = \prod_{\chi \in B} \langle \textstyle\sum_{t \in T'} \zeta^{pt} + \sum_{s \in S'} \zeta^s \,|\, \chi \rangle_{L/K} = \prod_{\chi \in B} \langle \textstyle\sum_{s \in S'} \zeta^s \,|\, \chi \rangle_{L/K} \in \mathfrak{p}^{f|B|}.
$$

Therefore (3) divides (4) and so $\prod_{\chi \in \widehat{G}} \langle \alpha \,|\, \chi \rangle_{L/K}$ divides $\prod_{\chi \in \widehat{G}} \langle \beta \,|\, \chi \rangle_{L/K}$ (note that $\widehat{G}$ is the disjoint union of A and B). Since $\beta \in \mathcal{O}_L$ was arbitrary, the desired result now follows from Corollary 4.4. $\qquad\square$

8. Proof of Theorem 1.2

We now prove an explicit version of Theorem 1.2. We adopt the notation given at the beginning of Section 7, taking $K = \mathbb{Q}^{(p^r)}$. We abbreviate $\langle - \,|\, \chi \rangle_{L/K}$ to $\langle - \,|\, \chi \rangle$.

Lemma 8.1. *Let $\chi \in B$ and define $a \in \mathbb{N}$ by $\chi(\sigma_{1+p^r}) = \zeta_{p^s}^a = \zeta^{ap^r}$. If $p = 3$, assume that $r \geq \min\{2, s\}$. Let $b \in V$. Then*

$$\mathrm{Norm}_{\mathbb{Q}^{(p^{r+s})}/\mathbb{Q}}((\langle \zeta^b \,|\, \chi \rangle)) = \begin{cases} p^{s(p-1)p^{r+s-1}} & \text{if } s \leq r \text{ and } v_p(b-a) \geq s, \\ p^{\frac{1}{2}(s+r)(p-1)p^{r+s-1}} & \text{if } s > r \text{ and } v_p(b-a) \geq r, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Exactly the same computation as in the proof of Lemma 7.4 gives

$$\langle \zeta^b \,|\, \chi \rangle = \zeta^b \sum_{j=0}^{p^s-1} \zeta^{p^r \left((b-a)j + bp^r \sum_{i=2}^{\lfloor s/r \rfloor+1} \binom{j}{i} p^{(i-2)r} \right)}.$$

Suppose $s \leq r$. Then using Lemma 5.2 for the second equality, we have

$$\langle \zeta^b \,|\, \chi \rangle = \zeta^b \sum_{j=0}^{p^s-1} \zeta^{p^r(b-a)j} = \begin{cases} \zeta^b p^s & \text{if } v_p(b-a) \geq s, \\ 0 & \text{otherwise.} \end{cases}$$

Suppose $s > r$. Let $l = v_p(b-a)$ and write $(b-a) = up^l$ where $(u, p) = 1$. If $l < r$, we have

$$\langle \zeta^b \,|\, \chi \rangle = \zeta^b \sum_{j=0}^{p^s-1} \zeta^{p^{r+l} \left((uj+bp^{r-l} \sum_{i=2}^{\lfloor s/r \rfloor+1} \binom{j}{i} p^{(i-2)r} \right)} = \zeta^b p^l \sum_{j=0}^{p^{s-l}-1} \zeta^{p^{r+l} \left((uj+bp^{r-l} \sum_{i=2}^{\lfloor s/r \rfloor+1} \binom{j}{i} p^{(i-2)r} \right)},$$

and so the result now follows from Corollary 5.8. On the other hand, if $l \geq r$ we have

$$\langle \zeta^b \,|\, \chi \rangle = \zeta^b \sum_{j=0}^{p^s-1} \zeta^{p^{2r} \left((up^{l-r}j + b \sum_{i=2}^{\lfloor s/r \rfloor+1} \binom{j}{i} p^{(i-2)r} \right)} = \zeta^b p^r \sum_{j=0}^{p^{s-r}-1} \zeta^{p^{2r} \left((up^{l-r}j + b \sum_{i=2}^{\lfloor s/r \rfloor+1} \binom{j}{i} p^{(i-2)r} \right)},$$

and so the result now follows by applying Corollary 5.10 with $k = s - r$, $e = r$ and rescaling appropriately. $\qquad\square$

Theorem 8.2. *Let p be an odd prime and let $r \geq 1$. If $p = 3$, assume that $r \geq \min\{2, s\}$. For $k \geq 1$, let*

$$R_k = \{(1 + c_1 p + c_2 p^2 + \ldots + c_{\min(r,k)-1} p^{\min(r,k)-1}) : 0 \leq c_i \leq p - 1\}$$

and let L_{r+k} be the unique subfield of $\mathbb{Q}^{(p^{r+k})}$ with $[\mathbb{Q}^{(p^{r+k})} : L_{r+k}] = p - 1$. For $s \geq 1$, let

$$\alpha_s = 1 + \sum_{k=1}^{s} \sum_{t \in R_k} \mathrm{Tr}_{\mathbb{Q}^{(p^{r+k})}/L_{r+k}}(\zeta_{p^{r+k}}^t) \quad and \quad G_s = \mathrm{Gal}(\mathbb{Q}^{(p^{r+s})}/\mathbb{Q}^{(p^r)}).$$

Then for all $s \geq 0$, we have $\mathcal{A}_{\mathbb{Q}^{(p^{r+s})}/\mathbb{Q}^{(p^r)}} = \mathcal{M}_{\mathbb{Q}^{(p^r)}[G_s]}$ and $\mathbb{Z}[\zeta_{p^{r+s}}] = \mathcal{A}_{\mathbb{Q}^{(p^{r+s})}/\mathbb{Q}^{(p^r)}} \cdot \alpha_s$. In other words, $\mathbb{Q}^{(p^{r+s})}/\mathbb{Q}^{(p^r)}$ is Leopoldt for all $s \geq 0$.

Proof. That $\mathcal{A}_{\mathbb{Q}^{(p^{r+s})}/\mathbb{Q}^{(p^r)}} = \mathcal{M}_{\mathbb{Q}^{(p^r)}[G_s]}$ is a straightforward application of Theorem 6.4 (i.e. the corollary to the main theorem in [BL96]).

We prove the main result by induction on s. The case $s = 0$ is trivial. Now fix $s \geq 1$ and assume by induction that $\mathbb{Z}[\zeta_{p^{r+s-1}}] = \mathcal{A}_{\mathbb{Q}^{(p^{r+s-1})}/\mathbb{Q}^{(p^r)}} \cdot \alpha_{s-1}$. Henceforth adopt the notation given at the beginning of Section 7, taking $K = \mathbb{Q}^{(p^r)}$. Let $\alpha = \alpha_s$ and $\gamma = \alpha_{s-1}$. Let $H = \{h_1, \dots, h_{p-1}\}$ be the unique subgroup of $\mathrm{Gal}(\mathbb{Q}^{(p^{r+s})}/\mathbb{Q})$ of order $p - 1$ and write $h_i = \sigma_{i+pf_i}$ for some $d_i \in \mathbb{Z}$. Let $S = \{(i+pf_i)x \mid x \in R_s\}$. Then observe that $\alpha = \gamma + \sum_{b \in S} \zeta^b$.

We wish to show that the hypotheses of Proposition 7.5 hold. Hypothesis (a) is the induction hypothesis and (b) holds by Lemma 8.1. Thus it remains to check (c).

Let $\chi \in B$. Then χ is of order p^s and there exists a unique $a \in V$ such that $0 < a < p^s$ and $\chi(\sigma_{1+p^r}) = \zeta_{p^s}^a = \zeta^{ap^r}$. We can write a uniquely as

$$a = (a_0 + a_1 p + a_2 p^2 + \dots + a_{s-1}p^{s-1}), \quad 0 \leq a_i \leq p - 1, \quad a_0 \neq 0.$$

Furthermore, there exists a unique element $c \in \mathbb{N}$ of the form

$$c = (1 + c_1 p + c_2 p^2 + \dots + c_{s-1}p^{s-1}) \quad 0 \leq c_i \leq p - 1$$

such that for $b := (a_0 + pf_{a_0})c$, we have $a \equiv b \bmod p^s$, i.e. $v_p(b - a) \geq s$.

Suppose that $s \leq r$. Then

$$R_s = \{(1 + d_1 p + d_2 p^2 + \dots + d_{s-1}p^{s-1}) : 0 \leq d_i \leq p - 1\}$$

and so b is the unique element of S such that $v_p(b - a) \geq s$. Hence by Lemma 8.1, b is the unique element of S such that $\langle \zeta^b \mid \chi \rangle \neq 0$, and so hypothesis (c) of Proposition 7.5 is satisfied in this case.

Suppose that $s > r$. Then

$$R_s = \{(1 + d_1 p + d_2 p^2 + \dots + d_{r-1}p^{r-1}) : 0 \leq d_i \leq p - 1\}.$$

There exists a unique $d \in R_s$ such that $v_p(d - c) \geq r$, namely

$$d = (1 + c_1 p + c_2 p^2 + \dots + c_{r-1}p^{r-1}).$$

Let $e = (a_0 + pf_{a_0})d \in S$. Since $v_p(a_0 + pf_{a_0}) = 0$, we have

$$v_p(e - b) = v_p((a_0 + pf_{a_0})(d - c)) = v_p(d - c) \geq r.$$

However, $a \equiv b \bmod p^s$ and so $v_p(e - a) \geq r$. By construction, e is the unique element of S with this property and therefore the property that $\langle \zeta^e \mid \chi \rangle \neq 0$ (use Lemma 8.1). Hence hypothesis (c) of Proposition 7.5 is satisfied in this case and so the proof is now complete. $\square$

Corollary 8.3. *Let $r, s \geq 1$ and p be an odd prime. If $p = 3$, assume that $r \geq \min\{2, s\}$. Let L/K be an extension with $[L : K] = p^s$ and $L \subseteq \mathbb{Q}^{(p^{r+s})}$. Then $\mathcal{A}_{L/K} = \mathcal{M}_{K[G]}$ and L/K is Leopoldt. In fact, if we suppose that L is of conductor p^{r+s} (which we can do without loss of generality) then $\mathcal{O}_L = \mathcal{A}_{L/K} \cdot \alpha_s$ for $\alpha_s \in \mathcal{O}_L$ as given in Theorem 8.2.*

Proof. That $\mathcal{A}_{L/K} = \mathcal{M}_{K[G]}$ is a straightforward application of Theorem 6.4 (i.e. the corollary to the main theorem in [BL96]).

Assume without loss of generality that L is of conductor p^{r+s}. Let L' and K' be the unique subfields such that $[\mathbb{Q}^{(p^{r+s})} : L'] = [\mathbb{Q}^{(p^r)} : K'] = p - 1$. The situation is illustrated by the field diagram below.
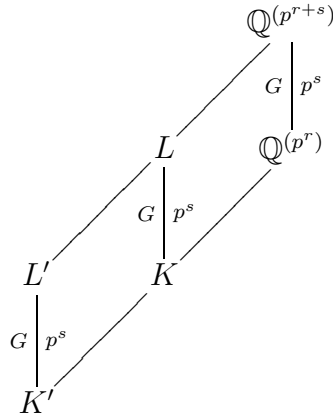
Since their degrees over K are relatively prime, $\mathbb{Q}^{(p^r)}$ and L are linearly disjoint over K. Furthermore, by definition of α_s in Theorem 8.2, it is easy to see that in fact $\alpha_s \in \mathcal{O}_{L'} \subseteq \mathcal{O}_L$. Hence the result now follows from Proposition 3.4 with $E = \mathbb{Q}^{(p^r)}$ and $F = \mathbb{Q}^{(p^{r+s})}$. $\square$

Corollary 8.4. *Let p be an odd prime and K be a subfield of $\mathbb{Q}^{(p)}$. Let*

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_\infty^{\mathrm{cyc}}$$

be the cyclotomic $\mathbb{Z}_p$-extension of K. Then for any $n \geq m$, the ring of integers $\mathcal{O}_{K_n}$ is free as a module over $\mathcal{A}_{K_n/K_m}$.

Proof. This is essentially just a rephrasing of Corollary 8.3. Recall Remark 7.1. $\square$

We can now deduce a theorem that is essentially the same as a result of Kersten and Michaliček ([KM89], Theorem 2.1). Also see [Gre92] and [Ich05].

Theorem 8.5. *Let p be an odd prime and K be any number field. Let*

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_\infty^{\mathrm{cyc}}$$

be the cyclotomic $\mathbb{Z}_p$-extension of K. For every $n \geq m$, the ring of p-integers $\mathcal{O}_{K_n}[p^{-1}]$ is free as a module over $\mathcal{O}_{K_m}[p^{-1}][\mathrm{Gal}(K_n/K_m)]$.

Proof. The main point is that p is inverted and since only primes above p are ramified in K_n/K_m, arithmetic disjointness outside of p is equivalent to linear disjointness. Hence the desired result can be obtained by base change from the case of Corollary 8.4. $\square$

9. Proof of Theorem 1.3

We now prove an explicit version of Theorem 1.3. We adopt the notation given at the beginning of Section 7, taking $K = \mathbb{Q}^{(p^r)+}$. We abbreviate $\langle - \,|\, \chi \rangle_{L/K}$ to $\langle - \,|\, \chi \rangle$.

Lemma 9.1. *Let $\chi \in B$ and define $a \in \mathbb{N}$ by $\chi(\sigma_{1+p^r}) = \zeta_{p^s}^a = \zeta^{ap^r}$. If $p = 3$, assume that $r \geq \min\{2, s\}$. Let $b \in V$. Then*

$$\mathrm{Norm}_{\mathbb{Q}^{(p^{r+s})}/\mathbb{Q}}((\langle \zeta^b \,|\, \chi \rangle)) = \begin{cases} p^{s(p-1)p^{r+s-1}} & \text{if } s \leq r \text{ and } \max\{v_p(b \pm a)\} \geq s \\ p^{\frac{1}{2}(s+r)(p-1)p^{r+s-1}} & \text{if } s > r \text{ and } \max\{v_p(b \pm a)\} \geq r, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. Observe that for any $k \geq 1$, we cannot have both $v_p(b - a) \geq k$ and $v_p(b + a) \geq k$, otherwise $v_p(b) = v_p(2b) = v_p((b - a) + (b + a)) \geq k$, contradicting the hypothesis on b. The result now follows immediately from Lemmas 7.3 and 8.1. $\qquad\square$

Theorem 9.2. *Let p be an odd prime and let $r \geq 1$. If $p = 3$, assume that $r \geq \min\{2, s\}$. For $k \geq 1$, let*

$$S_k = \{(c_0 + c_1 p + c_2 p^2 + \ldots + c_{\min(r,k)-1} p^{\min(r,k)-1}) : 0 \leq c_i \leq (p-1), 1 \leq c_0 \leq \tfrac{1}{2}(p-1)\}.$$

For $s \geq 1$, let

$$\alpha_s = \zeta_{p^r} + \sum_{k=1}^{s} \sum_{t \in S_k} \zeta_{p^{r+k}}^t \quad and \quad G_s = \mathrm{Gal}(\mathbb{Q}^{(p^{r+s})}/\mathbb{Q}^{(p^r)+}).$$

Then for all $s \geq 0$, we have $\mathbb{Z}[\zeta_{p^{r+s}}] = \mathcal{A}_{\mathbb{Q}^{(p^{r+s})}/\mathbb{Q}^{(p^r)+}} \cdot \alpha_s$. In other words, $\mathbb{Q}^{(p^{r+s})}/\mathbb{Q}^{(p^r)+}$ is Leopoldt for all $s \geq 0$.

Proof. We proceed by induction on s. In the case $s = 0$, it is trivial to check that $\alpha_0 = \zeta_{p^r}$ generates a normal integral basis for $\mathbb{Q}^{(p^r)}/\mathbb{Q}^{(p^r)+}$. Now fix $s \geq 1$ and assume by induction that $\mathbb{Z}[\zeta_{p^{r+s-1}}] = \mathcal{A}_{\mathbb{Q}^{(p^{r+s-1})}/\mathbb{Q}^{(p^r)+}} \cdot \alpha_{s-1}$.

Henceforth adopt the notation given at the beginning of Section 7, taking $K = \mathbb{Q}^{(p^r)+}$. Let $\alpha = \alpha_s$, $\gamma = \alpha_{s-1}$ and $S = S_s$. Then observe that $\alpha = \gamma + \sum_{b \in S} \zeta^b$. We wish to show that the hypotheses of Proposition 7.5 hold. Hypothesis (a) is the induction hypothesis and (b) holds by Lemma 9.1. Thus it remains to check (c).

Let $\chi \in B$. Then χ is of order $2p^s$ and there exists a unique $a \in V$ such that $0 < a < p^s$ and $\chi(\sigma_{1+p^r}) = \zeta_{p^s}^a = \zeta^{ap^r}$. We can write a uniquely as

$$a = (a_0 + a_1 p + a_2 p^2 + \ldots + a_{s-1} p^{s-1}), \quad 0 \leq a_i \leq p-1, \quad a_0 \neq 0.$$

Suppose that $s \leq r$. Then

$$S = \{(c_0 + c_1 p + c_2 p^2 + \ldots + c_{s-1} p^{s-1}) : 0 \leq c_i \leq (p-1), 1 \leq c_0 \leq \tfrac{1}{2}(p-1)\}.$$

Observe that $(S \uplus (-S)) \bmod p^s \equiv (\mathbb{Z}/p^s\mathbb{Z})^\times$ and so there exists a unique element $b \in S$ such that either $v_p(b - a) \geq s$ or $v_p(b + a) \geq s$. Hence by Lemma 9.1, b is the unique element of S such that $\langle \zeta^b \,|\, \chi \rangle \neq 0$, and so hypothesis (c) of Proposition 7.5 is satisfied in this case.

Suppose that $s > r$. Then

$$S = \{(c_0 + c_1 p + c_2 p^2 + \ldots + c_{r-1} p^{r-1}) : 0 \leq c_i \leq (p-1), 1 \leq c_0 \leq \tfrac{1}{2}(p-1)\}.$$

Observe that $(S \uplus (-S)) \bmod p^r \equiv (\mathbb{Z}/p^r\mathbb{Z})^\times$ and so there exists a unique $b \in S$ such that

$$\pm b \equiv (a_0 + a_1 p + \ldots + a_{r-1} p^{r-1}) \bmod p^r.$$

This is the unique element of S such that either $v_p(b - a) \geq r$ or $v_p(b + a) \geq r$ and so the unique element of S such that $\langle \zeta^b \,|\, \chi \rangle \neq 0$ (use Lemma 9.1). Hence hypothesis (c) of Proposition 7.5 is satisfied in this case and so the proof is now complete. $\square$

Remark 9.3. The idempotent $e = \frac{1}{2p^s}\mathrm{Tr}_{\mathbb{Q}^{(p^{r+s})}/\mathbb{Q}^{(p^r)+}}$ is in $\mathcal{M}_{\mathbb{Q}^{(p^r)+}[G_s]}$, but is not in $\mathcal{A}_{\mathbb{Q}^{(p^{r+s})}/\mathbb{Q}^{(p^r)+}}$ because $e(\zeta_{p^r}) = \frac{1}{2}(\zeta_{p^r} + \zeta_{p^r}^{-1}) \notin \mathbb{Z}[\zeta_{p^{r+s}}]$. Therefore $\mathcal{A}_{\mathbb{Q}^{(p^{r+s})}/\mathbb{Q}^{(p^r)+}} \subsetneqq \mathcal{M}_{\mathbb{Q}^{(p^r)+}[G_s]}$.

10. ACKNOWLEDGMENTS

REFERENCES

[BL96]   N. P. Byott and G. Lettl, *Relative Galois module structure of integers of abelian fields*, J. Théor. Nombres Bordeaux **8** (1996), 125–141.

[Ble95]   W. Bley, *A Leopoldt-type result for rings of integers of cyclotomic extensions*, Canad. Math. Bull. **38** (1995), 141–148.

[Bri87]   J. Brinkhuis, *Normal integral bases and complex conjugation*, J. reine angew. Math. **375/376** (1987), 157–166.

[Bri92]   ―――, *On the Galois module structure over CM-fields*, Manuscripta Math. **75** (1992), no. 4, 333–347.

[Bri94]   ―――, *On a comparison of Gauss sums with products of Lagrange resolvents*, Compositio Math. **93** (1994), no. 2, 155–170.

[CL93]   S.-P. Chan and C.-H. Lim, *Relative Galois module structure of rings of integers of cyclotomic fields*, J. reine angew. Math. **434** (1993), 205–220.

[Cou01]   J. Cougnard, *Nouveaux exemples d'extension relatives sans base normale*, Ann. Fac. Sci. Toulouse Math. (6) **10** (2001), no. 3, 493–505.

[CR81]   W. Curtis and I. Reiner, *Methods of representation theory with applications to finite groups and orders*, vol. 1, John Wiley & Sons, Inc., New York, 1981.

[Frö67]   A. Fröhlich, *Local fields*, Algebraic Number Theory (London) (J. W. S. Cassels and A. Fröhlich, eds.), Academic Press, 1967, pp. 1–47.

[Frö83]   ―――, *Galois module structure of algebraic integers*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), no. 1, Springer-Verlag, Berlin, 1983.

[FT91]   A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, no. 27, Cambridge Univ. Press, Cambridge, 1991.

[Góm96]   E. J. Gómez Ayala, *Normal bases for quadratic extensions inside cyclotomic fields*, Arch. Math. (Basel) **66** (1996), no. 2, 123–125.

[Gre92]   C. Greither, *Cyclic Galois extensions of commutative rings*, Lecture Notes in Mathematics, no. 1534, Springer-Verlag, Berlin, 1992.

[GRRS99] C. Greither, D. R. Replogle, K. Rubin, and A. S. Srivastav, *Swan modules and Hilbert-Speiser number fields*, J. Number Theory **79** (1999), no. 1, 164–173.

[Ich05]   H. Ichimura, *On the ring of p-integers of a cyclic p-extension over a number field*, J. Théor. Nombres Bordeaux **17** (2005), 779–786.

[Jac64]   H. Jacobinski, *Über die Hauptordnung eines Körpers als Gruppenmodul*, J. reine angew. Math. **213** (1964), 151–164.

[Jam]   M. James, *Class notes for Math 416, Galois modules (taught by L. R. McCulloh)*, http://www.math.uiuc.edu/∼mjames2/notes/.

[Joh06]   H. Johnston, *On the trace map between absolutely abelian number fields of equal conductor*, Acta Arith. **122** (2006), no. 1, 63–74.

[KM89]   I. Kersten and J. Michaliček, $\mathbb{Z}_p$-*extensions of complex multiplication fields*, J. Number Theory **32** (1989), no. 2, 131–150.

[Leo59]   H. W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. reine angew. Math. **201** (1959), 119–149.

[Let90]   G. Lettl, *The ring of integers of an abelian number field*, J. reine angew. Math. **404** (1990), 162–170.

[Let94]   _____, *Note on the Galois module structure of quadratic extensions*, Coll. Math. **67** (1994), 15–19.

[Let98]   _____, *Relative Galois module structure of integers of local abelian fields*, Acta Arith. **85** (1998), no. 3, 235–248.

[Mil]   J. Milne, *Algebraic number theory (Math 676)*, http://www.jmilne.org/math/.

[Nag51]   T. Nagell, *Introduction to number theory*, Wiley, 1951.

[Noe32]   E. Noether, *Normalbasis bei Körpern ohne höhere Verzweigung*, J. reine angew. Math. **167** (1932), 147–152.

[Rei75]   I. Reiner, *Maximal orders*, Academic Press, London-New York, 1975.

[Was97]   L. C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, no. 83, Springer-Verlag, New York, 1997.

Dept. of Math., Malott Hall, Cornell University, Ithaca, NY 14853-4201, USA

Current address: Fakultät für Informatik, Institut für theoretische Informatik und Mathematik, Universität der Bundeswehr München, 85577 Neubiberg, Germany

E-mail address: henri@math.cornell.edu

URL: http://www.math.cornell.edu/∼henri